802.11

Wireless Security Standards:

IEEE, IETF and NIST

Sheila Frankel
NIST

802.11 networks

- 802.11 Variants
  - 802.11b (2.4 GHz band – up to 11 Mbits/sec – up to 300 ft)
  - 802.11g (2.4 GHz band – 20+ Mbits/sec – up to 300 ft)
  - 802.11a (5 GHz band – up to 54 Mbits/sec – up to 80 ft)
- 802.11 Architectures
  - Centralized Wireless LAN: BSS (Basic Service Set)
    - AP (Access Point)
    - Stations
  - Ad hoc LAN: IBSS (Independent Basic Service Set)
- Additional Working Groups
  - 802.11i (Security)
  - 802.11c (QOS: Quality of Service)
  - 802.11r (Fast Roaming)
  - Management Frames Security Study Group

WEP: a flawed approach

- **Wired Equivalent Privacy**
- **Problematic encryption using RC4**
- **Flawed integrity protection using CRC**
- **Inadequate authentication**
- **No address protection**
- **No replay protection**
- **No key update mechanism**

TKIP: the short-term solution

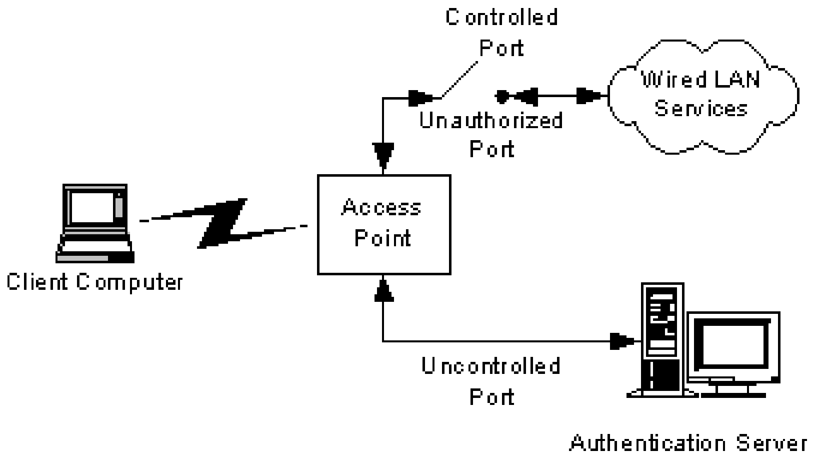
- Temporal Key Identity Protocol
- Constraints
- TKIP wrapper around RC4 for encryption
- Michael Keyed MIC (Message Integrity Code) for integrity protection
- IV-based sequence number for replay protection
- 802.1X for authentication and key management
- Software/firmware upgrade
- Subset adopted by WI-FI Alliance as WPA (Wi-Fi Protected Access)

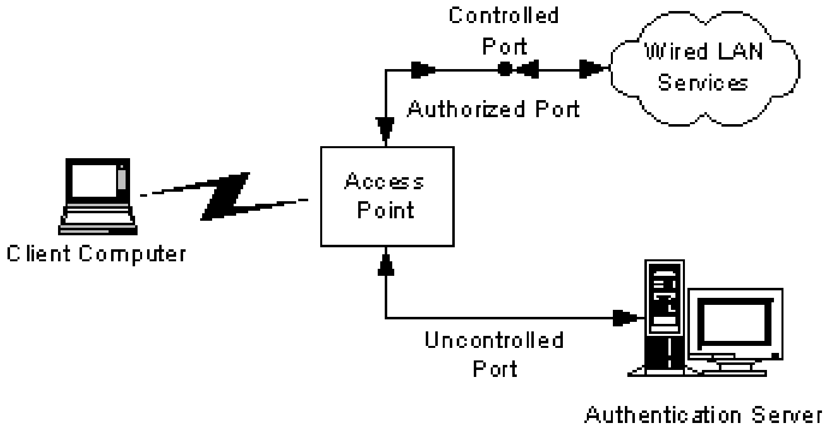
CCMP: the long-term solution

- Counter-Mode CBC-MAC Protocol (AES-based)
- AES-CTR (Advanced Encryption Standard in Counter mode) for encryption and integrity protection
- Packet sequence number for replay protection
- 802.1X for authentication and key management
- Requires more powerful hardware
- Also known as RSN (Robust Security Network)
- Adopted by WI-FI Alliance as WPA2

802.1X authentication: the missing piece

- **Port-based Network Access Control**
  - **Supplicant**
  - **Access point (AP)**
  - **Authentication server (AS)**





Authentication methods

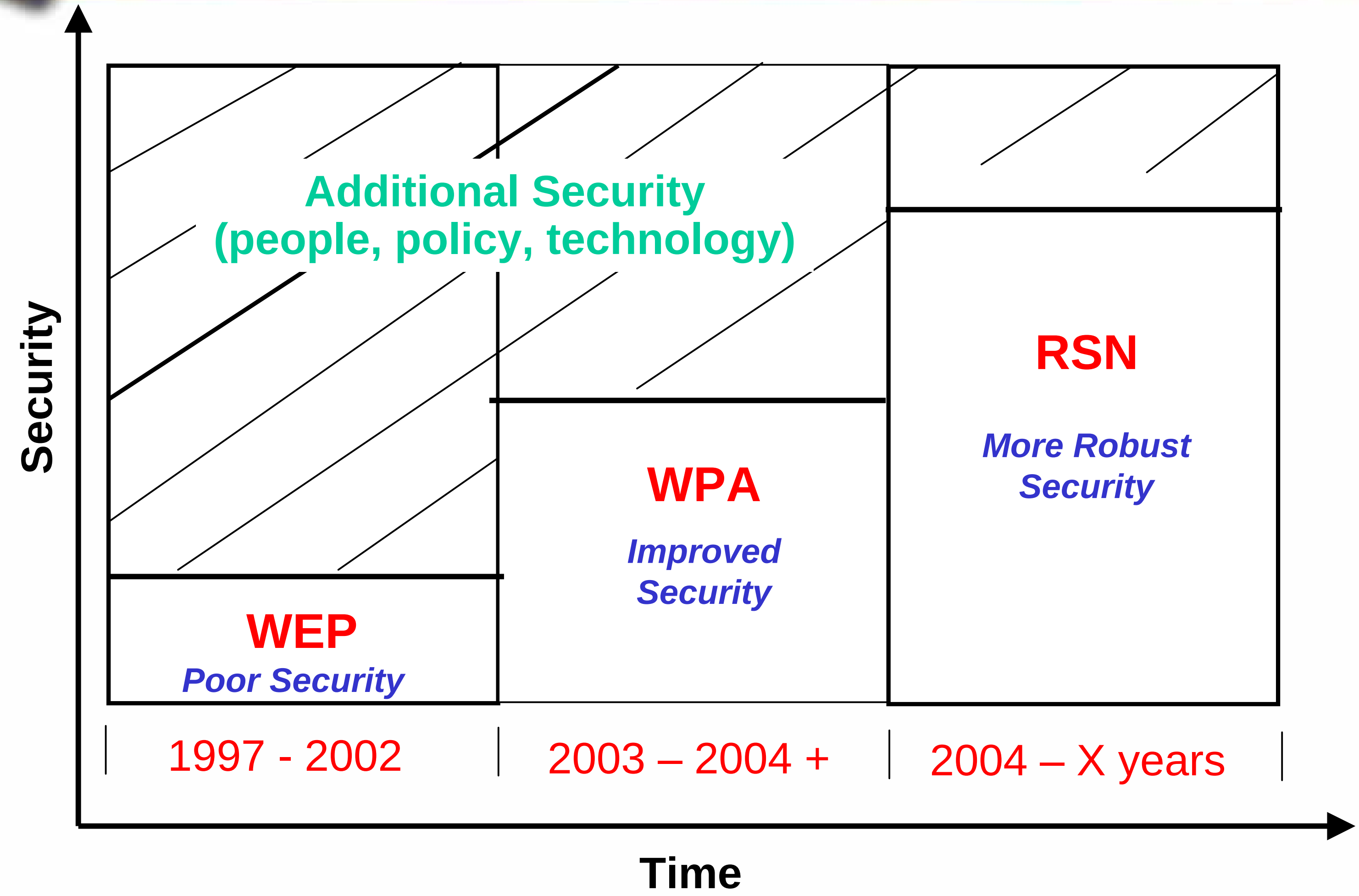
- Businesses: EAP (Extensible Authentication Protocol)
- Home user: PSK (Pre-shared key)
- Mutual authentication
- No single standardized EAP method selected for 802.11
- EAP-TLS (Transport Layer Security)
- EAP-TTLS (Tunneled Transport Layer Security)
- PEAP (Protected EAP)
- LEAP (Lightweight EAP)

Evolution of WiFi Security (IEEE)

Security Feature	Wired Equivalent Privacy (WEP)	WiFi Protected Access (WPA)	Robust Security Networks (RSN)
Encryption Algorithm	RC4	RC4	AES
Key Management	None	EAP-based	EAP-based
Cryptographic Keysize	40-bit or 104-bit	128-bit (64-bit for authentication)	128-bit
Packet Key	Created by Concatenation	Created by mixing function	Not needed
Data/Header Integrity	CRC-32 / None	Michael Algorithm	CCM
Cryptographic Key life	24-bit, wrap	48-bit	48-bit
Replay protection	None	Uses IV	Uses IV

Key: AES = Advanced Encryption Standard; CCM = Counter Mode with CBC-MAC (AES-based); EAP = Extensible Authentication Protocol; IV = Initialization Vector; RC4 = Rivest Cipher 4.

Standards-based WiFi Security Summary



Wireless Security Policy-related Challenges

- **Preventing mixed-mode operation**
- **Interoperability vs. proprietary features**
- **Adopting new technologies and enhanced uses/capabilities of existing technologies**
- **Security features in vendor products are frequently not enabled or can be easily disabled**
- **User education and re-education**
- **Timely response to device theft or misuse**
- **Long and arduous standards process**

NIST Wireless Initiatives

- Development of wireless security guidance documents
- Guidance and checklists for defining security-related policies
- Emerging wireless standards participation
- Wireless security research

- Empirical analysis in wireless Lab
- Explore impacts of technology convergence
- Technology assessments and secure architectures

Special Publication 800-48

- **“Wireless Network Security:**

  802.11, Bluetooth and Handheld Devices”
- **Examines the benefits and security risks of 802.11 WLAN, Bluetooth Ad Hoc Networks, and PDAs.**
- **Provides practical guidelines and recommendations for mitigating the risks associated with these technologies**
- **http://csrc.nist.gov/publications/nistpubs/**

  800-48/NIST_SP_800-48.pdf

Special Publication 800-xx

- “IEEE 802.11:

  Security for Next Generation Wi-Fi”

- In-depth examination of 802.11 security

- Best practices recommendations

- Case studies

Federal Information Processing Standard (140-2)

- **FIPS 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for federal agencies that have sensitive or valuable data (as defined in NIST Special Pub 800-21, Guideline for Implementing Cryptography in the Federal Government).**
- **This data must be protected through the use of FIPS-140-validated cryptography.**
- **Four levels of security (Level 4 is highest)**
- **Covers 11 topical areas (ports and interfaces, physical security, self-tests, finite state model, operational environment, etc.)**

- **As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.**
- **Must employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms.**

Contact

Sheila Frankel

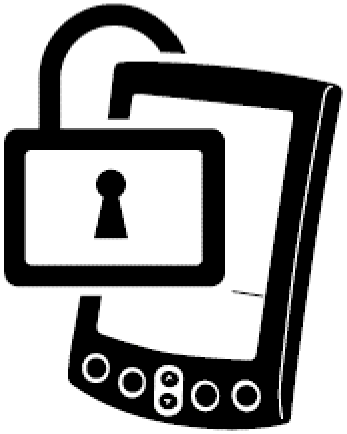
NIST

Computer Security Division

sheila.frankel@nist.gov

802.11 Security Checklist

802.11 Security Checklist



Threats and Vulnerabilities

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization’s computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.

Threats and Vulnerabilities

- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be introduced to a wired network connection.
- Malicious entities may connect to other organizations for the purposes of launching attacks and concealing their activity.
- Interlopers may be able to gain connectivity to network management controls and disrupt operations.

Management Countermeasures

- Identify who may use WLAN technology in an organization
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for APs
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed
- Define standard security settings for access points
- Describe limitations on how the wireless device may be used
- Describe the hardware and software configuration of any access device
- Provide guidelines on reporting lost devices and security incidents
- Provide guidelines on the use of encryption and other security software
- Define the frequency and scope of security assessments

Operational Countermeasures

- Maintaining a full understanding of the topology of the wireless network.
- Labeling and keeping inventories of the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.

Technical Countermeasures

- Updating default passwords.
- Establishing proper encryption settings.
- Controlling the reset function.
- Using MAC ACL functionality.
- Changing the SSID.
- Changing default cryptographic keys.
- Changing default SNMP Parameter.
- Disable remote SNMP. Use SNMPv3.
- Changing default channel
- Deploy personal firewalls and antivirus software on the wireless clients

Technical Countermeasures

- Test AP boundaries
- Intrusion Detection Systems
- Personal Firewalls
- Virtual Private Networks
- Consider other forms of authentication – RADIUS, Kerberos
- Complete Checklists for 802.11, Bluetooth, and Handheld devices are available in the guidance document.
- http://csrc.nist.gov